
UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA

v.

VADYM IERMOLOVYCH,
a/k/a "Vadim Ermolovich,"
a/k/a "Dima Ermolovich"
a/k/a "Dim,"
a/k/a "Dima,"
a/k/a "Dingos777,"
a/k/a "Vaer,"
a/k/a "Nadal,"
a/k/a "PriestTF,"
a/k/a "Kamazik"

: Hon. James B. Clark, III

: Mag. No. 14-3237 (JBC)

: CRIMINAL COMPLAINT

: **FILED UNDER SEAL**

I, Alexander Parisella, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent of the United States Secret Service, and that this complaint is based on the following facts:

SEE ATTACHMENT B

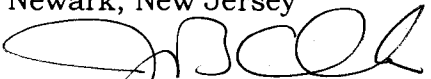
continued on the attached pages and made a part hereof.



Alexander Parisella, Special Agent
United States Secret Service

Sworn to before me, and
subscribed in my presence

November 5, 2014 at 12:04 pm
Newark, New Jersey



HONORABLE JAMES B. CLARK, III
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Count One
(Conspiracy to Commit Wire Fraud and Bank Fraud)

From at least as early as in or around October 2011 through in or around November 2012, in the District of New Jersey and elsewhere, defendant

VADYM IERMOLOVYCH,
a/k/a "Vadim Ermolovich,"
a/k/a "Dima Ermolovich,"
a/k/a "Dim,"
a/k/a "Dima,"
a/k/a "Dingos777,"
a/k/a "Vaer,"
a/k/a "Nadal,"
a/k/a "PriestTF,"
a/k/a "Kamazik"

did knowingly and intentionally conspire and agree with others to:

(1) devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communications in interstate commerce, certain writings, signs, signals, pictures, and sounds in a manner affecting a financial institution, contrary to Title 18, United States Code, Section 1343; and

(2) execute a scheme and artifice to defraud financial institutions, and to obtain moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of those financial institutions, by means of materially false and fraudulent pretenses, representations, and promises, contrary to Title 18, United States Code, Section 1344.

In violation of Title 18, United States Code, Section 1349.

Count Two
**(Conspiracy to Commit Fraud and Related Activity
in Connection with Computers)**

From at least as early as in or around October 2011 through in or around November 2012, in the District of New Jersey and elsewhere, defendants

VADYM IERMOLOVYCH,
a/k/a "Vadim Ermolovich,"
a/k/a "Dima Ermolovich,"
a/k/a "Dim,"
a/k/a "Dima,"
a/k/a "Dingos777,"
a/k/a "Vaer,"
a/k/a "Nadal,"
a/k/a "PriestTF,"
a/k/a "Kamazik"

did knowingly and intentionally conspire and agree with others to commit an offense against the United States, namely to intentionally access computers without authorization and exceed authorized access, and thereby obtain information from protected computers, that is, computers used in and affecting interstate and foreign commerce and communication, for purposes of commercial advantage and private financial gain, contrary to Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i).

In violation of Title 18, United States Code, Section 371.

ATTACHMENT B

I, Alexander Parisella, a Special Agent with the United State Secret Service ("USSS"), having conducted an investigation and discussed this matter with other law enforcement officers who have participated in this investigation, have knowledge of the following facts. Because this Criminal Complaint is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts which I believe are necessary to establish probable cause. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part. Where a particular statement is indicated to have been made in a different language, any quotations represent preliminary draft translations of such statements.

Background

1. At all times relevant to this Criminal Complaint, unless otherwise indicated:

Terms

a. "Skype" was an online communication service that allowed users to communicate using instant messaging, voice, or video chat.

b. "Structured Query Language," or "SQL," was a computer programming language designed to retrieve and manage data stored in computer databases.

c. "SQL Injection Attacks" were methods of hacking into and gaining unauthorized access to computers connected to the Internet.

Relevant Individuals and Entities

d. Defendant VADYM IERMOLOVYCH, a/k/a "Vadim Ermolovich," a/k/a "Dima Ermolovich," a/k/a "Dim," a/k/a "Dima," a/k/a "Dingos777," a/k/a "Vaer," a/k/a "Nadal," a/k/a "PriestTF," a/k/a "Kamazik," was a resident of Ukraine.

e. Co-conspirator "CC-1," not named as defendant herein, was a resident of Ukraine and a prolific computer hacker.

Victim Companies

f. The "Payment Card Victims" consisted of over 300 companies that maintained websites in industries such as finance, pharmaceutical, online gambling, adult, dating, and fashion.

The Scheme to Hack the Payment Card Victims

2. From at least as early as in or around October 2011 through in or around November 2012, in the District of New Jersey and elsewhere, CC-1 hacked into the computer networks of over 300 corporate victims, namely the Payment Card Victims, in order to steal credit and debit card data and related personal identifying information (collectively "Payment Card Data") for payment card accounts. Based upon the investigation, CC-1 relied heavily on SQL Injection Attacks, among various other methods and tactics, to infiltrate and navigate his victims' computer networks.

3. CC-1 then provided the stolen Payment Card Data to defendant IERMOLOVYCH and others, who resold the stolen data over the Internet and shared the proceeds with CC-1 and others involved in the scheme. In total, defendant IERMOLOVYCH acted as a reseller of such data for CC-1 and others, and trafficked and attempted to traffic in stolen Payment Card Data for approximately 600,000 payment card accounts.

4. In or around November 2012, law enforcement executed a number of searches in the Ukraine, including searches of computers and digital media located in CC-1's home. In connection with these searches, law enforcement seized, among other things, a laptop (the "CC-1 Computer"). From the CC-1 Computer, law enforcement recovered, among other things, online chat logs and remnants of online chats, active and deleted computer files, as well as internet search histories. The search also revealed that CC-1 maintained a meticulously organized directory of his hacking victims and kept copious notes regarding his/her hacking victims' vulnerabilities, and his/her progress in hacking their servers. CC-1 organized the majority of the stolen Payment Card Data within a directory called "work," and in two subdirectories called "CC" and "Carding." Within the "CC" subdirectory, CC-1 kept a unique folder for each of his hacking victims and targets. In addition for each victim, CC-1 maintained a "hack.txt" file containing notes regarding the methods he used to attempt and actually gain access to the Payment Card Victims. During the course of the conspiracy, the search of CC-1's computer revealed that CC-1 stole over approximately 773,000 pieces of Payment Card Data.

5. With respect to defendant IERMOLOVYCH, review of the chat logs from the CC-1 Computer revealed discussions between CC-1 and IERMOLOVYCH regarding their scheme to steal and sell Payment Card Data, as well as multiple instances of the actual transmission of stolen Payment Card Data from CC-1 to IERMOLOVYCH. For example:

a. Review of the CC-1 Computer confirmed that it was used to transmit over 18,000 pieces of stolen Payment Card Data obtained from the

Payment Card Victims, through Skype, to an account law enforcement has linked to defendant IERMOLOVYCH.

b. In an exchange occurring on or about October 23, 2012, defendant IERMOLOVYCH discussed certain pieces of the stolen Payment Card Data provided by CC-1. In this correspondence, defendant IERMOLOVYCH indicated that he had been purchasing stolen Payment Card Data from CC-1 for over a year.

6. In connection with the searches in Ukraine, law enforcement also seized a computer from defendant IERMOLOVYCH's home (the "Iermolovych Computer"). That search revealed over approximately 600,000 pieces of stolen Payment Card Data. Many of the approximately 18,000 stolen payment card numbers referenced above, and found on the CC-1 Computer, were also found on the CC-1 Computer.

7. The stolen Payment Card Data found on both the CC-1 Computer and the Iermolovych Computer included data related to multiple accounts belonging to thousands of individuals residing in the District of New Jersey. Additionally, the stolen Payment Card Data related to credit and debit cards issued by "financial institutions" as that term is defined in Title 18, United States Code, Section 20.

CC-1's Admissions to Law Enforcement

8. On or about March 19 and March 20, 2013, in connection with its investigation, law enforcement interviewed CC-1 in Ukraine (the "March 2013 Interviews"). At these interviews, CC-1 admitted that the CC-1 Computer belonged to him/her.

9. Search of the CC-1 Computer also revealed that on at least one occasion, on or about October 14, 2012, CC-1 used Skype to send stolen Payment Card Data to defendant IERMOLOVYCH in a compressed file that was password protected. At the March 2013 Interviews, CC-1 provided the password for the file. Law enforcement subsequently confirmed used the password to open the compressed file CC-1 sent to defendant IERMOLOVYCH, and confirmed its contents.